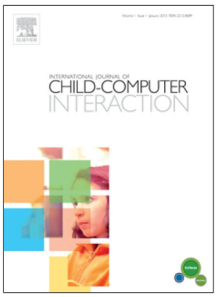
Journal Pre-proof



Age-appropriate password “best practice” ontologies for early educators and parents

Suzanne Prior, Karen Renaud

PII: S2212-8689(20)30004-0
DOI: https://doi.org/10.1016/j.ijcci.2020.100169
Reference: IJCCI 100169

To appear in: *International Journal of Child-Computer Interaction*

Received date : 14 November 2019
Revised date : 20 March 2020
Accepted date : 23 March 2020

Please cite this article as: S. Prior and K. Renaud, Age-appropriate password “best practice” ontologies for early educators and parents, *International Journal of Child-Computer Interaction* (2020), doi: https://doi.org/10.1016/j.ijcci.2020.100169.

Age-Appropriate Password "Best Practice" Ontologies for Early Educators and Parents

, Suzanne Prior[1] and Karen Renaud[1,2]
[1]Abertay University,UK [2]Rhodes University, South Africa

Abstract

Many mobile apps are developed specifically for use by children. As a consequence, children become actors in world where they use passwords to authenticate themselves from a very young age. As such, there is a need for guidance to inform educators and parents about how to prepare children for responsible password practice.

Very little attention has been paid to determining which password-related principles young children should know, and the age at which this information should be imparted. To address this deficiency, we commenced by deriving an ontology of "best practice" password principles from official sources. These password principles encode essential knowledge for password users of all ages and provide a benchmark that can be used to ground a set of age-appropriate ontologies.

We compared this benchmark "good practice" ontology to the advice provided by a wide-ranging snapshot of password-related children's books and parents' online resources. We then consulted the research literature to identify the skills required to understand and apply each principle, and removed those that were unsuitable for young children. We then consulted parents of young children to help us to confirm the classification of the ontology's principles in terms of age appropriateness. Parents also helped us to rephrase each principle to maximise accessibility and understandability for each age group.

We conclude with our final set of three *age-appropriate password best practice ontologies* as a helpful resource for early education professionals and parents.

1. Introduction

The use of digital technology by children has increased dramatically in recent years [1]. Systems designed specifically for children are becoming increasingly popular[1]. Primary school children have never known life without technology, and are increasingly using digital technology without supervision. Tablets are the most popular digital devices with 42% of children aged 5-7 owning their own tablet, compared to 5% for mobile phones [2]. Parents and teachers have a vital

[1]A search in February 2019 for "software for children" delivered 3,587K results

role to play in helping children to learn how to behave responsibly in the online world [3, 4, 5, 6].

Many of the applications used by children require them to authenticate themselves. Most developers of children's software use the password to authenticate children. Despite the increased interest in biometrics as an authentication method, many still believe that it will be necessary to use these alongside, not instead of, a password [7]. Moreover, there are understandable concerns related to the ethics of capturing and storing a child's biometric data [8].

The current situation is thus one where children are increasingly operating as independent agents in an online world, without necessarily having the requisite knowledge and skills to use passwords wisely [9, 10]. Children are not exempt from identity theft cyber attacks [11] so they need to be taught how to protect their information by engaging in responsible password practices.

In the absence of an ontology that can be used to inform child-related password "best practice" teaching, those who teach children about passwords understandably create and implement their own guidance and requirements. Studies have found that teachers value having standards to follow, to ensure that they teach the correct topics to their pupils [12, 13, 14]. There is also evidence that we cannot rely on parents to have the requisite understanding of good practice. For example, Livingstone *et al.* [15] report on an incident where parents shared passwords with their children, perhaps due to the parents themselves being unaware of best practice in this area, and not realising that they are setting a bad example.

We commence with a review of related research in Section 2, making the case for the development of age-appropriate ontologies. To address this need, we propose an evidence-based ontology to support both parents and teachers in communicating officially-grounded password "good practice" to children.

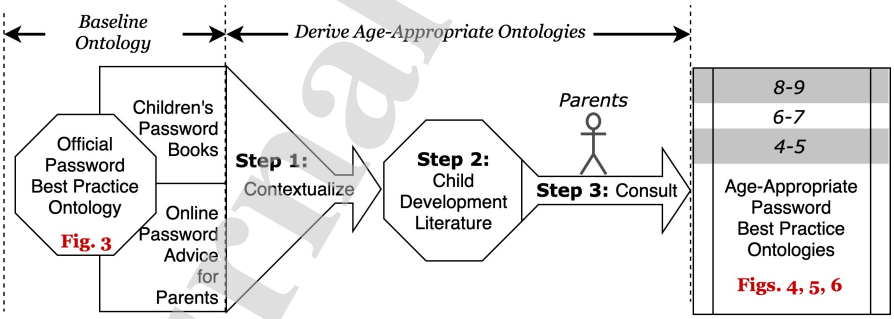


Figure 1: Overview of the Reported Research

Our research methodology is depicted in Figure 1. The first step was to develop an understanding of exactly what the state of password "best practice" guidance is. To determine this, we derived an ontology of best practice from documents published by official standards bodies (Section 3). The next step was to consider what advice children and parents currently have access to in

children's books and online documents (Section 4) and to compare these to the derived best practice ontology. Section 5 explains how we worked with educators and parents to produce three age-appropriate password "best practice" ontologies for the age groups: 4-5, 6-7 and 8-9. Section 6 concludes.

2. Related Research

The UK's Information Commissioner's office published age-appropriate design guidelines [16], which says: "*The best interests of the child should be a primary consideration when you design and develop online services likely to be accessed by a child*" (p.24). Authentication is something every online service user engages with, regardless of their age. We are required, therefore, to consider the child's authentication needs, as well as those of adults.

O'Brien [17] highlights the lack of approved cybersecurity curricula for primary schools, which confirms the need for the research reported in this paper. Some notable studies have indeed focused on children's password behaviours and mental models of passwords. Most academic studies of under 18's understanding of cyber principles have focused on teenagers [18, 19] yet some have indeed focused on younger children.

Read and Cassidy [20] carried out an investigation into how children created textual passwords. They provide some design guidelines for software aimed at children. Yet Dempsey *et al.* [21] argue that the guidelines would produce software that is too easy to compromise, while acknowledging that those systems not using these guidelines could lead children to use coping skills, such as writing down passwords.

Choong *et al.* [9] reviewed all the literature related to children and passwords since the year 2000, only one of which reports children's knowledge of passwords [22]. Choong *et al.* [9] subsequently carried out a study with American children, to determine understanding of password principles. They reported that children were somewhat confused about why they needed passwords, with many referring to privacy and safety rather than security. While passwords are certainly *necessary* in assuring privacy and child safety they are not sufficient in this respect. A number of other measures work together with passwords to assure privacy and safety.

Many of the younger children needed help creating passwords, which highlights the need for the role of responsible adults to be included within the ontologies. This is confirmed by Kumar *et al.* [18]. Relatively few of Choong *et al.'s* child participants (12.5%) admitted writing down their passwords while 54% of Ratakonda *et al.'s* [10] child participants also doing this. A third of Choong *et al.'s* participants reported sharing their passwords, as did 68% of Ratakonda *et al.'s* child participants. Many of Choong *et al.'s* participants mentioned reusing passwords for multiple accounts, as did 8 out of 22 of Ratakonda *et al.'s* child participants.

Lamichhane and Read [23] used an Android game to study password and username creation with young children, aged 7 and 8. They discovered that most children used passwords that were six characters long. Most also used the

names of familiar items in their passwords. This suggests high guessability, and this is confirmed by Maqsood's [19] study with older children (aged 11-13). Read and Cassidy [20] report on a child shouting their password across a classroom, evidencing a lack of understanding of the need for password security.

Chartofylaka and Delcroix [24] developed a game to teach children password principles and report a positive impact in terms of teaching children about stronger passwords. They encourage use of lowercase, uppercase, digits and symbols (LUDS) in passwords though, which is now considered suboptimal [25]. Hundlani *et al.* [26] developed a way for parents to log in on their children's behalf, which is an innovative tool, but at some stage children have to learn to function responsibly in the online world [27], and then they will need to know password "good practice" principles.

These studies confirm the need for age-appropriate password good practice ontologies, and this need is also highlighted by both Kumar *et al.* [18] and Livingstone *et al.* [15]. The ontology we derive in this paper will act as a foundation for further work in this area, all moving towards a more grounded password-related education for young children.

3. A Password "Best Practice" Ontology

An ontology: "*defines a common vocabulary for researchers who need to share information in a domain. It includes machine-interpretable definitions of basic concepts in the domain and relations among them*" [28, p.1].

Ontologies have been developed in cyber for digital forensics [29, 30], cyber investigations [29], cyber defence systems [31]. risk management [32] and more general cyber security principles [33, 34]. In creating our benchmark ontology, we followed the *methontology* approach proposed by Fernández *et al.* [35]. We worked through each of their stages, as follows:

3.1. Specification

Domain: Authentication
Purpose: Ontology about password principles to be understood by a password user.
Level of Formality: Informal
Scope: List of password-related concepts from an end user perspective.
Sources of Knowledge: Official reports including the National Institute of Standards and Technology (NIST) [25], the Centre for the Protection of National Infrastructure [36] and the UK government [37].

3.2. Conceptualisation

The conceptualisation was achieved as follows: we searched for official guidance from the UK and other governments. These included guidance directly from the UK and USA government and from organisations linked to them. We worked through the documents and created a card for each concept, redundancy was achieved very quickly with these documents. We then worked together to

cluster concepts into groups so that we were able to identify relevant concepts, instances, verbs and properties. Only aspects that directly related to the end user control were included.

We classified the advice into one of three categories, and seven subcategories, as follows:

1. *Password Understanding:*
   (a) **W**hy Passwords? (W_i)
   (b) **P**assword **I**ssues (PI_i);
   (c) **P**assword **L**eakage **C**onsequences (PLC_i);
2. *Good Practice Application:*
   (a) **P**assword **C**reation (PC_i);
   (b) **P**assword **R**etention (PR_i);
   (c) **P**assword **E**ntry (PE_i);
3. ***P**assword **T**ools* (PT_i).

For each password issue, we included the mitigating behaviour under one of the application-related behaviours (see Figure 2). We only included the one PLC: "Impersonation". Many consequences could occur as a result of a password being leaked, but all stem from impersonation.

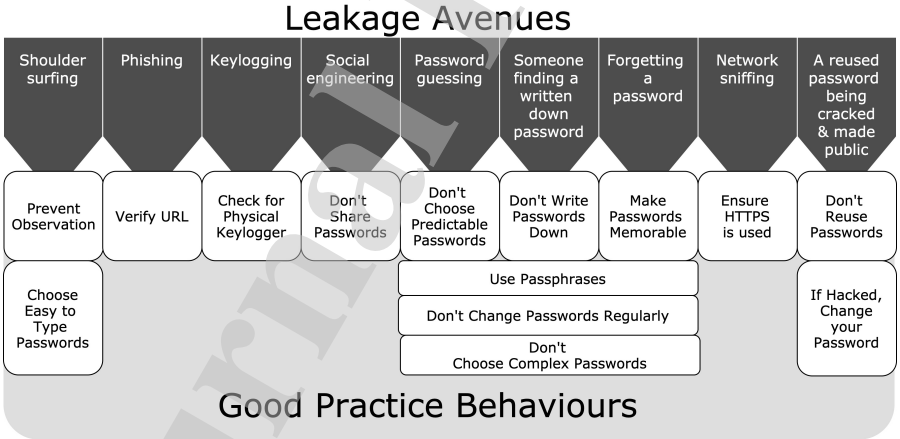


Figure 2: Mapping Leakage Avenues to Behaviours

3.3. Integration

Since the other cyber security ontologies did not include password-relevant concepts, we were not able to integrate any existing ontology concepts.

3.4. Implementation

We depicted the ontology concepts and their relationships in diagrammatic format to facilitate evaluation.

3.5. Evaluation

We recruited six cyber security experts, using convenience sampling, based on our personal contacts. We asked for their help in confirming the advice to be included in the ontology. We gave them the headings (password creation, password retention, etc.) and asked them to help us add principles under each category. The experts had not seen the created ontology at this point. We grouped their suggestions to identify themes. Three concepts emerged that had not been included in our ontology. Unfortunately, none of these were in keeping with the latest guidance:

- LUDS: use of Lowercase, Uppercase, Digits and Symbols;
- Passwords should be changed frequently;
- Write them down in one place.

What struck us was the level of disagreement amongst the experts, something we did not anticipate. This exercise did not add any new "good practice" principles to the ontology.

We then asked two more cyber security experts to evaluate our ontology. The first was an academic teaching in the area of cyber security, the second a chief security officer a large company who also had primary school teaching experience. The final refined ontology, which incorporates their suggestions and refinements, is shown in Figure 3.

4. Comparison to Extant Advice

Having derived a "foundational" ontology, we wanted to compare the password principles parents and children were being exposed to, to assess the coverage and correctness of the principles in children's books an online resources.

4.1. Advice from Children's Books

There are many resources available to parents and educators wishing to improve children's knowledge on a range of topics. However, the physical book still remains an important resource, especially in Scotland, where this research was carried out. The Scottish Book Trust gifts a selection of books to every child on four occasions between birth and age five[2] to encourage children to enjoy reading. Other countries are likely to have similar schemes, and most primary schools still have libraries.

[2] https://www.scottishbooktrust.com

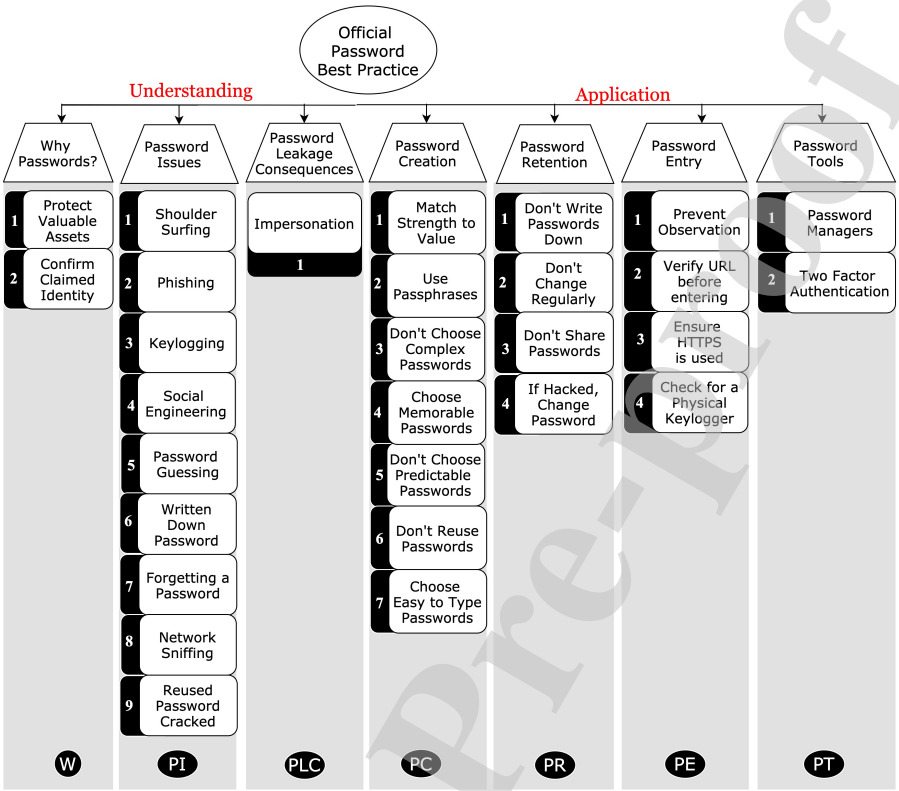


Figure 3: Password "Best Practice" Ontology

Retrieving Books: We searched for books aimed at children, which provided password-related guidance. To find books we visited the UK's national bookseller (Waterstones), as a first step. They had a wide range of cyber bullying and cyber safety books, but none that dealt with password-related principles. We then searched for books on amazon.com, amazon.co.uk, ebay.co.uk, ebay.com and second-hand bookshops. We purchased paper copies of relevant books, and downloaded Kindle books. We visited our city's local public library and searched their catalogues. We retrieved a total of 21 books, of which 6 were discarded because, despite seeming applicable, they did not include password best practice guidance. See Tables 1 and 2.

Table 1: Reasons for Book Rejection

Books	**Reason**
[38, 39, 40, 41]	There is no mention of passwords within the book.
[42, 43]	Book is aimed at adults not children.

Table 2: Books Used in Ontology (F=Fiction;NF=Non Fiction)

Book Title & Author	**Year**	
Internet Safety by Josepha Sherman [44]	2003	NF
Internet Safety — Kids' Guide by Victoria Roddel [45]	2006	NF
Keep Your Passwords Secret by Shannon Miller [46]	2014	NF
Passwords and Security by Eric Minton [47]	2014	NF
Lizzy's Triumph over cyber-bullying by Nina Du Thaler [48]	2015	F
Understanding Computer Safety by Paul Mason [49]	2015	NF
Usbourne Staying Safe Online by Jennifer Perry, Felicity Brooks [50]	2016	NF
The Magic Zablet by James Gosnold [51]	2016	F
Lucy's Family Launches into the Cyber World by Nina Du Thaler [52]	2017	F
Dot.Common Sense by Ben Hubbard [53]	2018	NF
A focus on...online safety by Steffi Cavell-Clarke [54]	2018	NF
Passwords Are Secret by Anthony Ardely [55]	2018	NF
Staying Safe Online by Steffi Cavell-Clarke [56]	2018	NF
Safety and Security by Ben Hubbard [57]	2018	NF
Sharing Passwords Featuring Peggy the Parrot by Dave Stanley and Sandrijn Stead [58]	2019	F

Findings Table A.4 shows each book's coverage of the official guidelines.

The books contain 26 items of advice, as compared to 29 within the official guidance. On average, the books contained 10.9 (SD = 6.8) references of information in 8.2 (SD=4.3) categories. Fiction books contained, on average, five (SD = 2) references to information in 4.3 (SD = 1.15) categories. Non Fiction books contained on average 12.7 (SD = 6.7) references to information in 9.4 (SD = 4.2) categories. Table A.5 shows the aggregate coverage of official guidelines by the children's books.

The books contained seven items of guidance that was ambiguous, out of date and/or incorrect. For example, children were advised not to write down passwords, but were also advised on ways of doing so securely. The majority of books advise the use of LUDS (lowercase, uppercase, digit and special characters) when creating passwords, whereas the official guidance rules that this is no longer "good practice" [25]. In the case of some books, this is likely to be because the books were published before this guidance appeared. However it is interesting to note that even the most recent books contained this advice. This serves to highlight some of the challenges in presenting up to date cyber security information.

Three categories relate to incorrect information on trust: readers were advised to work with other people to create passwords and in some cases to work with "an older friend". The main threat within books was that of strangers (i.e. someone who might hurt them). This might cause children to conflate security and safety, which is bound to cause problems later on.

Children are also advised to change their passwords frequently, another piece

of advice that is no longer considered good practice [25]. None of the books suggested an essential piece of advice: "match password strength to value" (PC1). By this, we mean that a bank account password should be much stronger than a password that protects a newspaper subscription, for example. Of course "value" here is personal. To a child, a game might be very important and they would want to keep their siblings out of their game, whereas for an adult the same game might be unimportant.

4.2. Online Guidance

We searched for documents outlining password principles for children, using Google.co.uk, on the 18th March 2020. We analysed all the hits on the first two pages because very few people go beyond the first page returned by an Internet search engine [59]. This makes it likely that the majority of parents will focus on these first two pages of results. This snapshot gives us a sense of the advice that is available online, to compare to our official ontology. A search for "*password advice for children*" returned no results. A *children and "password principles"* returned 341 results. Eighteen of the links on the first two pages were not relevant to children, and one was a link to a Bachelor's Thesis reporting on password behaviours on the entire age range, from age 10 to retirement [60]. The final link incorrectly recommended LUDS passwords, as well as frequent password changes to children [61]. The third search we carried out was for *children and "password advice"*. This returned 34K results. On the first two pages, one link gave advice to teachers managing passwords for their classes [62] and the rest (19) did not provide child-specific advice.

The final search for "*password advice for children*" returned 161 million results, being the most fruitful. The following advice was provided via the links in the first two pages:

Why passwords? [63, 64]

Password Issues: (1) Consequences of leaked passwords [65, 66, 67]; (2) Phishing [64]; (3) Keylogging [64].

Password Creation: (1) {Incorrect} LUDS advice for creation[3] [65, 68, 69, 67]; (2) Don't choose predictable passwords [68, 66, 63, 69, 64]; (3) Use a passphrase [68]; (4) Don't reuse passwords [68, 66, 67]; (5) Create memorable passwords [69].

Password Retention: (1) Don't write them down [65, 68, 66]; (2){Incorrect} Change passwords often [66, 69]; (3) Change password if it has been leaked [64]; (4) It's ok to share with Mum and Dad [63, 69].

Password Tools: (1) Password managers [65, 68, 64]; (2) Two factor authentication [68]; (3) Don't share passwords [65, 66, 63, 69, 64].

Password Entry: Check the site's URL before entering the password [65];

There were also links to advice for University students and adults[4], for par-

[3] https://www.youtube.com/watch?v=9LxdtaSvQ3I

[4] https://www.connectsafely.org/passwords/;https://us.norton.com/internetsecurity-how-to-how-to-secure-your-passwords.html

ents in keeping their children safe online[5] and password manager adverts. One linked to a password generator for children[6].

Findings: The online sources offered advice, once we arrived at the right search term. Some of the advice was incorrect, and the coverage was not as broad as that of the children's books. Online sources, like the children's books, also incorrectly advised the use of LUDS and frequent password changes. Some also tell children that passwords are required for privacy and online safety, which is not entirely accurate. While passwords control access to accounts, they do not, in and of themselves, guarantee privacy and online safety. An important new category of advice emerged i.e. *parental role*, which is useful in addressing the role of the educator in our context of use. This can be included in lesson plans when delivering the child-specific ontology principles.

4.3. Reflection

The differences between the official ontology (Figure 3) and the offered advice (children's books and online sources) are reflected in Table A.5. We can now highlight noteworthy differences.

Strangers and Friends: Both fiction and non-fiction books often contained the suggestion or idea that a hacker is a stranger, linked to the "stranger danger" idea often contained within children's education. However, within cyber security, this is inaccurate. A child is at risk of hacking from both known *and* unknown persons. Many children's charities advise that parents know their child's passwords in order to monitor their activities online and to protect them from abuse [70]. This is often depicted in books as sharing a password with a *person you trust*. This could be a confusing message: they are likely to trust their best friend, but sharing their password with their best friend is neither appropriate nor advisable.

Recency of Guidance: Cyber security is a fast evolving field and, as a consequence, password creation and management guidance is changing at a faster rate than most other guidance. The oldest book in our study was from 2003, with the majority being from 2015 or later. It is clearly impossible for a physical book to stay current in this domain yet even the Kindle books we reviewed did not present current advice.

The online advice was also somewhat out of date, advising password complexity and frequent password changes. Moreover, some sources argue that passwords deliver privacy and guarantee safety, both of which are inaccurate.

Summary: Those wishing to develop educational resources, such as books in the area of cyber security, need to consider the challenge of keeping pace with the changing environment. Online sources are much easier to keep current and updated, but this requires continuous engagement and effort, and our investigation suggested that this is not happening as often as it should. When a resource

[5] https://us.norton.com/internetsecurity-kids-safety-stop-stressing-10-internet-safety-rules-to-help-keep-your-family-safe-online.html

[6] https://www.dinopass.com/

reflects good practice in a fast moving field, it has to be reviewed at regular intervals, and this has to be scheduled, and the next revision date noted within the existing document. It is infeasible for books to be able to achieve this, and our snapshot review suggests that online sources also do not keep their advice current.

5. Deriving an Age-Appropriate Password "Best Practice" Ontology

The ontology depicted in Figure 3 is essentially context independent. While this is a strength when it comes to informing adult behaviours, it is a flaw when it comes to the ontology being a resource for teachers. Our focus is on "good practice" password principles to be taught to children as they move through the early education schooling system.

In deriving age-appropriate ontologies for the three age groups, we did the following:

Step 1. Scrutinize each of the principles in the official ontology. Remove those that are inappropriate for children aged 9 and under. Add new ones that are required to tailor the ontology for use by educators and parents.

Step 2. Consult the child development literature to identify the skills required to apply each "good practice" password principle.

Step 3. Consult parents to:

(a) identify the principles that they consider their child, aged 4-9, would reasonably be able to understand and apply.

(b) rephrase the text of the identified principles so that they will be understood by a child of the targeted age.

5.1. Step 1: Contextualise Principles

We first added a new item to "Password Creation" (PC8), which instructed the child to speak to his/her Teacher, Carer, Mummy or Daddy if they were unsure of anything. We removed too advanced and too abstract principles, as follows:

1. ***Too Advanced:***

   (a) ***PC3:*** *Don't Choose Complex Passwords:* this advice does not align with the way young children are taught, because negation is an advanced and complex concept [71]. Children are taught *what* to do, not told what *not* to do. Moreover, PC2 refers to the use of passphrases, which is essentially the equivalent of this piece of advice, phrased positively. A passphrase focuses on the length of the authentication text, as opposed to a concentration on lowercase, uppercase, digits and symbols [25]. Hence PC3 is both inappropriate and superfluous.

(b) ***PT1 & PT2:*** *Password Tools:* the ontologies are targeted at under 9s, which makes the teaching of password tools premature.

2. ***Too Abstract:*** Ausubel [72] explains that primary school children depend on prior concrete-empirical experience to develop their understanding of new concepts. That being so, too-abstract principles, or those that the child is unlikely to have direct experience of, are unlikely to be accessible to under 9s. Hence the following "good practice" principles were not included in our age-appropriate ontologies.

   (a) ***PI8:*** *Network Sniffing:* network sniffing is a complicated concept. The ability to prevent it often lies with the administrator of a network — it is not a concept which children would be able to understand or control their risk for.

   (b) ***PE4 & PI3:*** *Keylogging:* most keylogging takes place via software, which is invisible and impossible to spot. This piece of advice is unhelpful, even for adults.

   (c) ***PI2 & PR2:*** *Phishing:* many adults fall for Phishing so it might seem worth teaching children about Phishing and checking URLs, even at a young age. However, Google will only give an email account to children aged 13 or over, so that it might be too soon to teach under 9s these principles. Moreover, the checking of URLs requires a child to be able to combine several skills, literacy, problem solving, value judgements and attention. This is likely to be beyond the capabilities of the age ranges we are targeting.

We now consider the abilities required to support application of the remaining principles.

5.2. Step 2: Required Abilities

We commenced with the skills mentioned by [73] in their password life cycle. Then, with the help of a developmental psychologist, we considered each item in the best practice ontology presented in Figure 3 to enumerate the required cognitive skills needed by the child to apply each piece of advice. A number of necessary cognitive skills were identified as being required in order to apply the good practice principles. A child may understand a concept without being able to apply it, so we do not consider PI_i here.

Literacy: Ehri [74] proposed a staged reading model in 1995. She argues that children go through four stages of development: (1) pre-alphabetic, (2) partial alphabetic, (3) full alphabetic, and (4) consolidated alphabetic. Beech [75] explains that Ehri's stages assume eventual automatic reading as an adult reader. Since passwords are essentially complicated sequences of alphabetic symbols, children cannot be expected to use text passwords until they are fluent readers. However, it is almost impossible to predict the age at which children will reach Ehri's 4th stage, although we can argue that children aged 4-5 are

unlikely to be full alphabetic. This means that children aged 4-5 cannot be expected to apply principles: PC2, PC7, PR1, PE2 and PE3.

Focus: Children spend years learning to read and building vocabulary. Certainly they cannot read at an adult level till they reach adolescence, and this will influence their password choices. Children are frequently taught to spell through phonological decoding [76], and to recognise words through this and other scaffolding techniques, such as examination of adjacent words [77]. Both of these approaches rely on a child being able to see the word that they are typing to ensure it is correct. It also assumes that the password being entered is a known word, as opposed to a series of random characters. This impacts on the type of password which can be used by the child, and the length of password which is realistic for them to enter. This means that PC7 is contra-indicated for the youngest children. PE1 might also be problematic since it adds an extra cognitive load as they are trying to enter their password [78, 79]

Creativity, problem solving, decision making, and attention: Children differ in their ability to focus attention on a particular task. Differences have been attributed to bilingualism [80], gender [81] and dyslexia [82], to mention but three. This, in turn, will influence their ability to problem solve, be creative and make decisions [83], impacting the password generation stage.

Gathercole [84] explains that the capacity to retain information improves drastically as children age. She also explains that speech-based memory is linked to literacy levels. Since passwords are often words, this suggests a link between the retention of passwords and literacy levels. Sowell [85] explains that children do not reach adult levels of retention ability until adolescence. Hence they might well have difficulties retaining a password, especially if multiple character types are involved.

When someone enters a password, they have to be able to type the password and be able to track the position in the password mentally. We were not able to find any studies on children's ability to enter password correctly in the absence of visual feedback. It is likely to be linked to attentional and literacy abilities.

This category has particular relevance when it comes to password creation and password retention. The literature is clear about the fact that there is great variability with respect to age and these abilities, so for these principles we will need to find a way to communicate the principles in a way that does not require these skills at a mature level. We will thus rely on Step 3's parent consultation to formulate the principles in a way that is accessible to under 9s. Certainly, it is clear that the first age group, 4-5, is unlikely to have the skills required to apply principles requiring these skills, including PC3, PC4, and PC5.

Secret keeping from peers: Peskin & Ardino [86] find that children do indeed know how to keep secrets by the age of 5, and that this improves with age. On the other hand, they are likely to share their secrets with their friends [87]. Because they are likely to give a password if asked, we ought to teach them specifically how to respond to such requests rather than trying to forbid sharing. However, given that the age of 5 is mentioned, this means that secret-related good practice principles (PR3 and PR4) ought not to be taught to the first age group.

Value judgements: This might require children to make value judgements, something which usually develops by 8 years of age [88], but one can expect there to be some variation in this, as in any other childhood development. This means that good practice principles PC1 and PC5 should not be introduced to the first two age groups.

Thinking about thinking & understanding others: Educational and developmental psychologists would probably approach many of these concepts from a meta-cognition [89] and/or theory of mind [90] perspective. However, since children are being required to use passwords long before they have matured sufficiently, we have to rely on parents and teachers finding a way to communicate these somewhat abstract good practice principles to children before they have mastered these skills.

5.3. Step 3: Parent Consultation

To ensure that the ontology components were formulated and delivered in an age-appropriate way, we recruited parents of children in the three different age groups: 4-5, 6-7 and 8-9. We asked our external relations team to publicise our request for assistance and 12 parents from across our institution volunteered to help us to validate our ontology contents, formulate the phrasing and finalise the ontologies.

We asked the parents to help us to formulate each component in a child-friendly and understandable way, and also to help us fix on the age at which they ought to be able to apply it. We gave each parent a sheet of A3 sized paper, with sections labelled '4-5', '6-7' and '8-9'. Having recorded their child's age, we asked them to identify the good practice principles that they considered their child would be able to understand and apply. We also asked them how they would communicate that principle to their child.

We then compared the ages they chose for each principle to those that we derived from the literature (Step 2). There were some differences, which we dealt with as follows:

1. PE1 is related to being observed while entering the password. The parents of 4-5 year olds thought their children would be able to check for observers *before* commencing, conflicting with what the literature suggested. However, being aware of observation *while* entering their password is clearly something 4-5 year olds could not yet do. We thus tailored PE1 for the 4-5 year olds, and upgraded it for the later years to include checking for observers both before and during password entry.

2. PR3 and PR4 are both related to password leakage, and the parents pointed this out. To simplify matters, we combined and simplified these as follows: "*If someone knows your password, change it*".

5.4. Summary

Table A.3 summarises the age-appropriate ontology derivation process, showing which good practice principles were removed, and how those that were retained were allocated to each of the three different ontologies.

Based on their inputs, we produced three ontologies, one for each age group, which we present in Figures 4, 5 and 6.

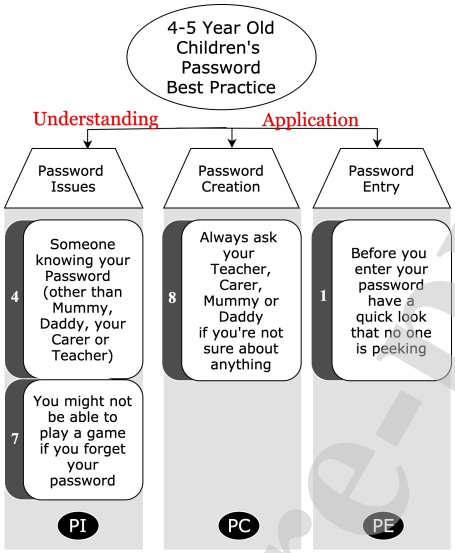


Figure 4: Password Good Practice for 4-5 Year Olds

5.5. Reflection

We strove to develop age-appropriate password "best practice" principles as a resource for primary school teachers, especially those who teach under 9s. As we derived these, two findings were particularly surprising:

Expert Disagreement: While the official sources we consulted to derive the ontology depicted in Figure 3 agreed on all points, the experts we consulted did not. Some advocated the use of passwords managers, while others did not. Some advocated LUDS passwords, others recommended the use of passphrases. Before NIST and the NCSC published their guidelines, the use of LUDS was accepted good practice, and it seems that these outdated guidelines have become ingrained. This confirms previous research related to people struggling to abandon a habitual practice [91, 92].

The dominance of LUDS in Books and Online Sources: The overwhelming majority of the books and online sources issued this advice, essentially recommending complexity. While it is understandable that books become outdated, we were rather surprised at the online courses also issuing this advice. We expected online advice to be more current, but this was not the case.

These insights highlight *firstly* the need for everyone to go on refresher courses, when it comes to a dynamic field such as cybersecurity. Good practice in this domain is not static, and we have to make an effort to keep up. *Secondly*, it also highlights the need for organisations to keep their own educational

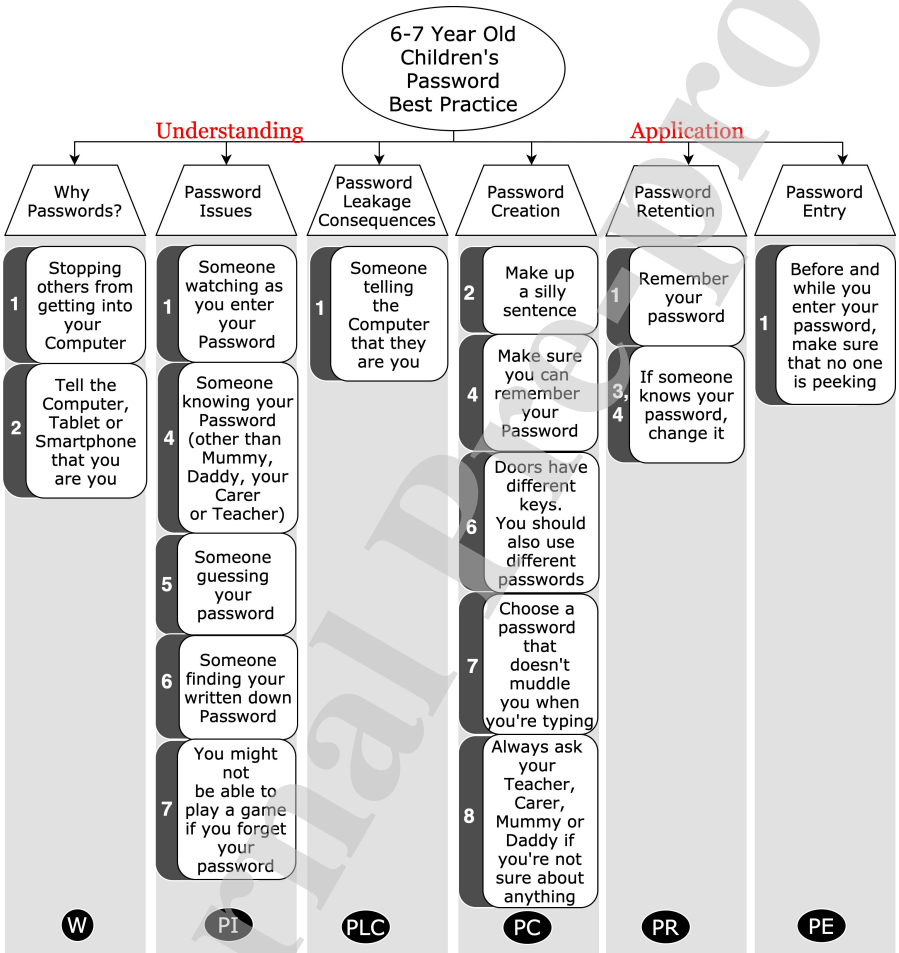


Figure 5: Password Good Practice for 6-7 Year Olds

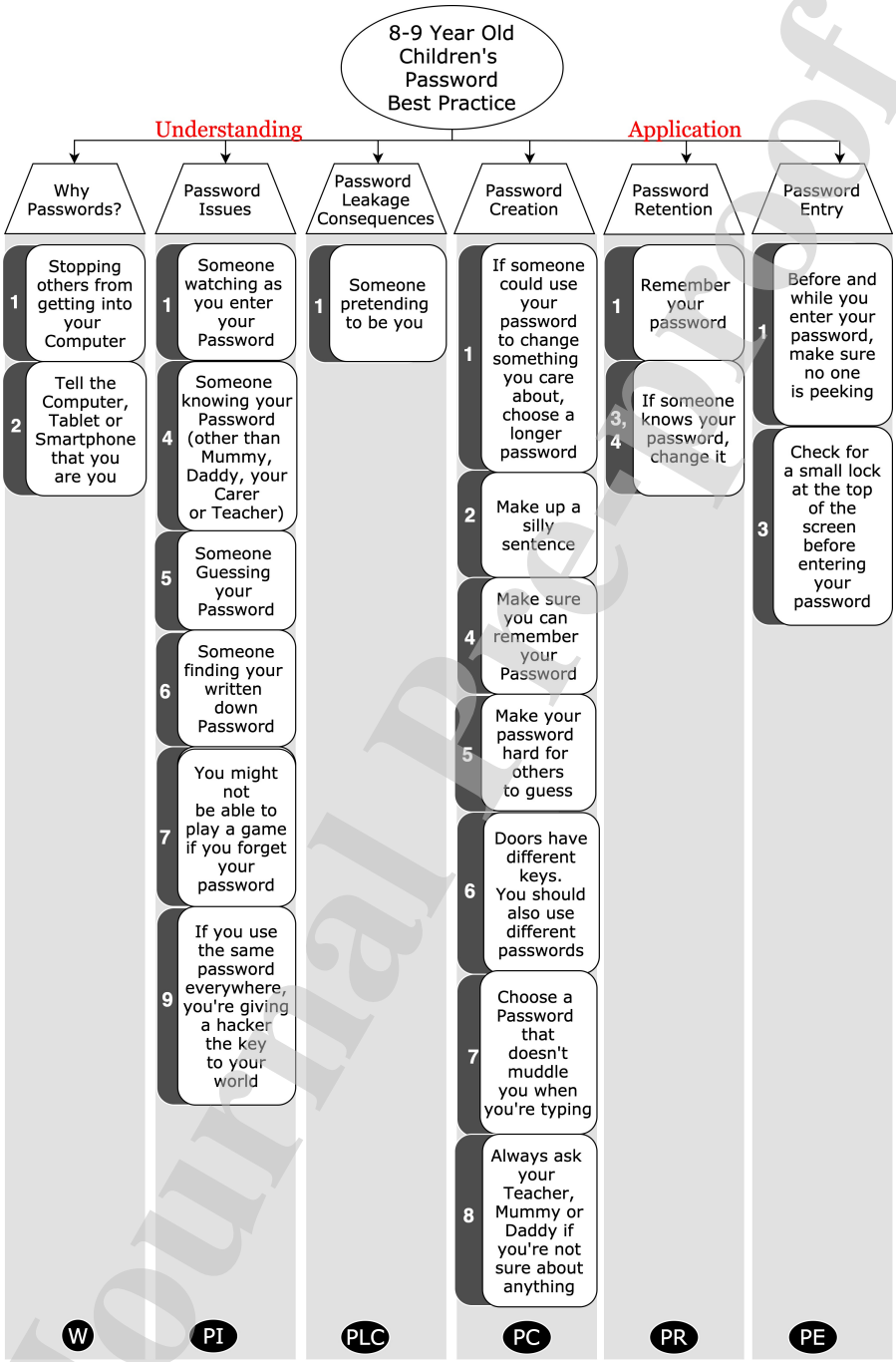


Figure 6: Password Good Practice for 8-9 Year Olds

materials current so that they do not unwittingly issue outdated advice, which could lead to insecure behaviours.

6. Conclusion and Future Work

It is essential for children to learn good practice at the outset, because it is very difficult to get people to change the way they manage their passwords after poor practice has become entrenched, as was demonstrated when we consulted out experts.

Technology has been embraced by society and by schools, and there is a need to include password-related skills in the school curriculum. We have derived a child-centred ontology of password "good practice" to help educators impart the right principles to children at the right age. To ensure maximum efficacy, we provide three *age-appropriate ontologies*. Parents and educators can use these to ensure that children are taught principles as and when they are ready to comprehend and apply them. We are currently working on developing lesson plans for educators, to help them to deliver the best practice principles to their charges.

Acknowledgements

We thank our colleagues in the Division of Cyber Security for always being willing to discuss our research with us — their help has been invaluable. We also thank Lara Wood for her help in considering the impact of children's developmental stages. Finally, we thank the parents of young children for helping us to verify the three age-appropriate ontologies.

References

[1] D. Holloway, L. Green, S. Livingstone, Zero to eight: Young children and their Internet use, EU Kids Online. LSE London, EU Kids Online, eprints.lse.ac.uk/52630 (2013).

[2] Ofcom, Children and parents media use and attitudes 2018, https://www.ofcom.org.uk/research-and-data/media-literacy-research/childrens/children-and-parents-media-use-and-attitudes-report-2018 Accessed 18 July 2019 (2018).

[3] Her Majesty's Government, Horizon Scanning Programme: Social attitudes of young people, www.gov.uk/government/uploads/system/uploads/attachment_data/file/389086/Horizon_Scanning_-_Social_Attutudes_of_Young_People_report.pdf Accessed August 2019 (2014).

[4] M. M. Terras, J. Ramsay, Family digital literacy practices and children's mobile phone use, Frontiers in Psychology 7 (2016) 1957.

[5] I. Beyens, K. Beullens, Parent–child conflict about children's tablet use: The role of parental mediation, New Media & Society 19 (12) (2017) 2075–2093.

[6] P. Nikken, S. J. Opree, Guiding young children's digital media use: SES-differences in mediation concerns and competence, Journal of Child and Family Studies 27 (6) (2018) 1844–1857.

[7] N. Kobie, Surveillance State: Fingerprinting pupils raises safety and privacy concerns, The Guardian https://www.theguardian.com/sustainable-business/2016/feb/19/surveillance-state-fingerprinting-pupils-safety-privacy-biometrics Accessed 18 July 2019 (Feb 2016).

[8] B. Patton, The trouble with taking biometric technology into schools, The Conversation, http://theconversation.com/the-trouble-with-taking-biometric-technology-into-schools-52355 Accessed 18 July 2019 (2016).

[9] Y.-Y. Choong, M. Theofanos, K. Renaud, S. Prior, Case Study – Exploring Children's Password Knowledge and Practices, in: Usable Security (USEC). San Diego, February, 2019.

[10] D. K. Ratakonda, T. French, J. A. Fails, "My Name is My Password:" Understanding Children's Authentication Practices, in: Proceedings of the 18th ACM International Conference on Interaction Design and Children, June 12–15, Boise, ID, USA, 2019, pp. 501–507.

[11] R. D. Tiwari, An Analytical Study on the Awareness of Parents about Cybercrimes against Children, International Journal on Transformations of Media, Journalism & Mass Communication (Online ISSN: 2581-3439) 4 (2) (2019).

[12] A. M. Metz, Teaching statistics in biology: using inquiry-based learning to strengthen understanding of statistical analysis in biology laboratory courses, CBE—Life Sciences Education 7 (3) (2008) 317–326.

[13] K. Appleton, How do beginning primary school teachers cope with science? Toward an understanding of science teaching practice, Research in Science Education 33 (1) (2003) 1–25.

[14] W. Harlen, Primary teachers' understanding in science and its impact in the classroom, Research in Science Education 27 (3) (1997) 323.

[15] S. Livingstone, G. Mascheroni, M. Dreier, S. Chaudron, K. Lagae, How parents of young children manage digital devices at home: The role of income, education and parental style, http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EUKidsIV/PDF/Parentalmediation.pdf Accessed September 2019 (2015).

[16] Information Commissioner's Office, Age appropriate design: a code of practice for online services, https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/ Accessed 18 March 2020 (2020).

[17] C. O'Brien, Teachers' perceptions about use of digital games and online resources for cybersecurity basics education: A case study, Ph.D. thesis, Capella University (2019).

[18] P. Kumar, S. M. Naik, U. R. Devkar, M. Chetty, T. L. Clegg, J. Vitak, 'No Telling Passcodes Out Because They're Private': Understanding Children's Mental Models of Privacy and Security Online, Proc. ACM Hum.-Comput. Interact. 1 (CSCW) (2017) 64:1–64:21, http://doi.acm.org/10.1145/3134699. doi:10.1145/3134699.

[19] S. Maqsood, Children's Text Password Behaviors and Parental Advice, Master's thesis, Computer Science, Carleton University (2018).

[20] J. C. Read, B. Cassidy, Designing textual password systems for children, in: Proceedings of the 11th International Conference on Interaction Design and Children, ACM, Bremen, Germany, 2012, pp. 200–203.

[21] J. Dempsey, B. Cassidy, G. Sim, Child-centered security, in: BCS Learning and Development Ltd. Proceedings of British HCI 2016 Conference Fusion, Bournemouth, UK, 2016, pp. 1–3.

[22] P. E. Coggins III, Implications of what children know about computer passwords, Computers in the Schools 30 (3) (2013) 282–293.

[23] D. R. Lamichhane, J. C. Read, Investigating children's passwords using a game-based survey, in: Proceedings of the 2017 Conference on Interaction Design and Children, IDC '17, ACM, Stanford, California, USA, 2017, pp. 617–622. doi:10.1145/3078072.3084333.

[24] L. Chartofylaka, A. Delcroix, StoryPass–Password Rules Hidden in a Storytelling Game Activity: Steps towards Its Implementation, in: 8th International Toy Research Association World Conference, Paris, France, 2018.

[25] P. A. Grassi, J. L. Fenton, E. M. Newton, R. A. Perlner, A. R. Regenscheid, W. E. Burr, J. P. Richer, N. B. Lefkovitz, J. M. Danker, Y.-Y. Choong, K. K. Greene, M. F. Theofanos, NIST Special Publication 800-63B, Digital Identity Guidelines, Tech. rep., NIST, https://pages.nist.gov/800-63-3/sp800-63b.html Accessed September 2019 (2017).

[26] K. Hundlani, S. Chiasson, L. Hamid, No passwords needed: The iterative design of a parent-child authentication mechanism, in: Proceedings of the 19th International Conference on Human-Computer Interaction with Mobile Devices and Services, MobileHCI '17, ACM, Vienna, Austria, 2017, pp. 45:1–45:11. doi:10.1145/3098279.3098550.

[27] J. Guan, J. Huck, Children in the digital age: Exploring issues of cybersecurity, in: Proceedings of the 2012 iConference, ACM, Toronto, Ontario, Canada, 2012, pp. 506–507. doi:10.1145/2132176.2132266.
URL http://doi.acm.org/10.1145/2132176.2132266

[28] N. F. Noy, D. L. McGuinness, Ontology development 101: A guide to creating your first ontology, Tech. Rep. KSL-01-05, Stanford Knowledge Systems Laboratory Technical Report (2001).

[29] H. Park, S. Cho, H.-C. Kwon, Cyber forensics ontology for cyber criminal investigation, in: International Conference on Forensics in Telecommunications, Information, and Multimedia, Springer, 2009, pp. 160–165.

[30] A. Brinson, A. Robinson, M. Rogers, A cyber forensics ontology: Creating a new approach to studying cyber forensics, Digital Investigation 3 (2006) 37–43.

[31] N. Ben-Asher, A. Oltramari, R. F. Erbacher, C. Gonzalez, Ontology-based Adaptive Systems of Cyber Defense., in: Semantic Technology for Intelligence, Defense, and Security (STIDS), Fairfax VA, USA, 2015, pp. 34–41.

[32] A. Oltramari, D. S. Henshel, M. Cains, B. Hoffman, Towards a Human Factors Ontology for Cyber Security., in: Semantic Technology for Intelligence, Defense, and Security (STIDS), Fairfax VA, USA, 2015, pp. 26–33.

[33] A. Oltramari, L. F. Cranor, R. J. Walls, P. D. McDaniel, Building an Ontology of Cyber Security., in: Semantic Technology for Intelligence, Defense, and Security (STIDS), Fairfax VA, USA, Citeseer, 2014, pp. 54–61.

[34] L. Obrst, P. Chase, R. Markeloff, Developing an Ontology of the Cyber Security Domain., in: Semantic Technology for Intelligence, Defense, and Security (STIDS), Fairfax VA, USA, 2012, pp. 49–56.

[35] M. Fernández-López, A. Gómez-Pérez, N. Juristo, Methontology: from ontological art towards ontological engineering, Tech. rep., AAAI Technical Report SS-97-06 (1997).

[36] Centre for the Protection of National Infrastructure, Password guidance: Simplifying your approach, Tech. rep., National Technical Authority for Information Assurance (CESG), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/458857/Password_guidance_-_simplifying_your_approach.pdf Accessed September 2019 (2015).

[37] UK Government, Ask users for passwords, https://design-system.service.gov.uk/patterns/passwords/ (undated).

[38] M. Masters, Hawkeye Collins and Amy Adams in The Case of the Clever Computer Crooks and 8 Other Mysteries, Meadowbrook Books, 1983.

[39] L. Palin, Super Cybersecurity Grandma: Episode 3 - Privacy and Identity Theft, Jastin Enterprises, Maryland, 2017.

[40] T. Orr, Cyber Citizenship and Cyber Safety Privacy and Hacking, Rosen Publishing, 2008.

[41] I. AlQasem, Freaky Rivet Online Safety for Kids, Nabilsi, 2015.

[42] M. Peesel, Internet Safety for Children - A Parent's Practical Guide to Keeping their Children Safe Online, Notable Publishing Inc, 2013.

[43] M. Ribble, Raising a Digital Child, HomePage Books, 2009.

[44] J. Sherman, Internet Safety, Watts Library, USA, 2003.

[45] V. Roddel, Internet Safety Kids' Guide, Lulu Press, USA, 2006.

[46] S. Miller, Keep Your Passwords Secret, Power Kids Press, New York, USA, 2014.

[47] E. Minton, Passwords and Security, Power Kids Press, New York, USA, 2014.

[48] N. Du Thaler, Lizzy's Triumph Over Cyber-bullying!: Cyber safety can be fun, Bright Zebra, ebook, 2015.

[49] P. Mason, Understanding Computer Safety, Raintree, London, UK, 2015.

[50] F. B. Jennifer Perry, Usboure Staying Safe Online, Usbourne, London, UK, 2016.

[51] J. Gosnold, The Magic Zablet: A story about Cyber Security, for the next generation, CreateSpace Independent Publishing Platform, ebook, 2016.

[52] N. Du Thaler, Lucy's family launches into the cyber-world!: Cyber safety can be fun, Bright Zebra, ebook, 2017.

[53] B. Hubbard, Dot.Common Sense How to stay smart and safe online, Wayland, London, UK, 2018.

[54] S. Cavell-Clarke, A focus on...online safety, Book Life, King's Lynn, UK, 2018.

[55] A. Ardely, Passwords Are Secret, PowerKids Press, New York, USA, 2018.

[56] S. Cavell-Clarke, T. Welch, Staying Safe Online, Booklife Publishing, King's Lynn, UK, 2018.

[57] B. Hubbard, My Digital Safety and Security, Franklin Watts, London, UK, 2018.

[58] D. Stanley, S. Stead, Sharing Passwords Featuring Peggy the Parrot, Independently Published, 2019.

[59] E. Cutrell, Z. Guan, What are you looking for? An eye-tracking study of information usage in web search, in: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM, San Jose, California, 2007, pp. 407–416.

[60] A. Bjöorneskog, N. G. Shoshtari, Comparison of Security and Risk awareness between different age groups, Blekinge Institute of Technology (2014).

[61] B. Hopper, Moms: 10 Must-See Ways to Keep Your Kids Safe on Facebook, https://backgroundchecks.org/moms-10-must-see-ways-to-keep-your-kids-safe-on-facebook.html Accessed 18 July 2019 (2013).

[62] I. Addison, How do you manage passwords with primary school children?, https://www.e-safetysupport.com/stories/5/how-do-you-manage-passwords-with-primary-school-children Accessed 18 March 2020 (2013).

[63] Get Safe Online, Protecting Passwords, https://www.getsafeonline.org/safeguarding-children/protecting-passwords/ Accessed 18 March 2020 (2019).

[64] UK Council for Internet Safety, Education for a Connected World, https://www.gov.uk/government/publications/education-for-a-connected-world Accessed 18 March 2020 (2019).

[65] Marvin the Robot, Naivety — the wrong way to behave on the Internet, https://usa.kaspersky.com/blog/security-tips-for-kids-2/5611/ Accessed 18 March 2020 (2015).

[66] M. McGraw, 9 Online Password Safety Tips To Teach Your Kids, https://scrapsofmygeeklife.com/geek-stuff/online-password-safety-tips-kids/ Accessed 18 March 2020 (2012).

[67] N. Feather, The age of cybersecurity is forcing parents to redefine "the talk"?, https://qz.com/1764777/how-to-talk-to-your-kids-about-cybersecurity/ Accessed 18 March 2020 (2020).

[68] L. B. Stevens, Safe Password Tips Your Child Should Know, https://wezift.com/parent-portal/blog/safe-password-tips-your-child-should-know/ Accessed 18 March 2020 (2020).

[69] Common Sense Media, What are some good rules for screen names and passwords?, https://www.commonsensemedia.org/privacy-and-internet-safety/what-are-some-good-rules-for-screen-names-and-passwords Accessed 18 March 2020 (2014).

[70] Get Safe Online, Protecting passwords, https://www.getsafeonline.org/safeguarding-children/protecting-passwords/ (2019).

[71] R. Mayo, Y. Schul, E. Burnstein, "I am not guilty" vs "I am innocent": Successful negation may depend on the schema used for its encoding, Journal of Experimental Social Psychology 40 (4) (2004) 433–449.

[72] D. P. Ausubel, The transition from concrete to abstract cognitive functioning: Theoretical issues and implications for education, Journal of Research in Science Teaching 2 (3) (1964) 261–266.

[73] Y.-Y. Choong, A cognitive-behavioral framework of user password management lifecycle, in: International Conference on Human Aspects of Information Security, Privacy, and Trust, Springer, Heraklion, Crete, 2014, pp. 127–137.

[74] L. C. Ehri, Phases of development in learning to read words by sight, Journal of Research in Reading 18 (2) (1995) 116–125.

[75] J. R. Beech, Ehri's model of phases of learning to read: a brief critique, Journal of Research in Reading 28 (1) (2005) 50–58.

[76] K. Strattman, B. W. Hodson, Variables that influence decoding and spelling in beginning readers, Child Language Teaching and Therapy 21 (2) (2005) 165–190.

[77] B. A. Murray, M. J. McIlwain, C.-h. Wang, G. Murray, S. Finley, How do beginners learn to read irregular words as sight words?, Journal of Research in Reading 42 (1) (2019) 123–136.

[78] J. W. Hagen, G. A. Hale, The development of attention in children., ERIC, 1973.

[79] J. Wilding, F. Munir, K. Cornish, The nature of attentional differences between groups of children differentiated by teacher ratings of attention and hyperactivity, British Journal of Psychology 92 (2) (2001) 357–371.

[80] E. Bialystok, S. Majumder, The relationship between bilingualism and the development of cognitive processes in problem solving, Applied Psycholinguistics 19 (1) (1998) 69–85.

[81] M. Raffaelli, L. J. Crockett, Y.-L. Shen, Developmental stability and change in self-regulation from childhood to adolescence, The Journal of Genetic Psychology 166 (1) (2005) 54–76.

[82] C. Peyrin, M. Lallier, J.-F. Demonet, C. Pernet, M. Baciu, J. F. Le Bas, S. Valdois, Neural dissociation of phonological and visual attention span disorders in developmental dyslexia: FMRI evidence from two case reports, Brain and Language 120 (3) (2012) 381–394.

[83] H. A. Simon, G. B. Dantzig, R. Hogarth, C. R. Plott, H. Raiffa, T. C. Schelling, K. A. Shepsle, R. Thaler, A. Tversky, S. Winter, Decision making and problem solving, Interfaces 17 (5) (1987) 11–31.

[84] S. E. Gathercole, Cognitive approaches to the development of short-term memory, Trends in Cognitive Sciences 3 (11) (1999) 410–419.

[85] E. R. Sowell, P. M. Thompson, C. M. Leonard, S. E. Welcome, E. Kan, A. W. Toga, Longitudinal mapping of cortical thickness and brain growth in normal children, Journal of Neuroscience 24 (38) (2004) 8223–8231.

[86] J. Peskin, V. Ardino, Representing the mental world in children's social behavior: Playing hide-and-seek and keeping a secret, Social Development 12 (4) (2003) 496–512.

[87] L. Anagnostaki, M. J. Wright, A. Papathanasiou, Secrets and disclosures: How young children handle secrets, The Journal of Genetic Psychology 174 (3) (2013) 316–334.

[88] A. Schlottmann, Children's probability intuitions: Understanding the expected value of complex gambles, Child Development 72 (1) (2001) 103–122.

[89] S. Larkin, Metacognition in young children, Routledge, 2009.

[90] H. M. Wellman, The child's theory of mind., The MIT Press, 1992.

[91] K. Renaud, B. Otondo, M. Warkentin, "This is the way 'I' create my passwords" ... does the endowment effect deter people from changing the way they create their passwords?, Computers & Security 82 (2019) 241–260.

[92] D. Ariely, M. I. Norton, How actions create - not just reveal - preferences, Trends in Cognitive Sciences 12 (1) (2008) 13–16.

Appendix A. Tables

Table A.3: Summary of the Derivation Process (V=Value judgements; L=Literacy; C=Creativity; F=Focus; S=Secret keeping)

	Step 1	Step 2	Step 3 Appropriate Age			
	Context	Skills	4-5	6-7	8-9	Notes
W1				•		
W2				•		
PI1				•		
PI2	⊠					
PI3	⊠					
PI4			•			
PI5				•		
PI6				•		
PI7			•			
PI8	⊠					
PI9					•	
PLC				•		
PC1		≥8 (V)			•	
PC2		≥6 (L)		•		
PC3	⊠					
PC4		≥6 (C)		•		
PC5		≥8 (VC)			•	
PC6				•		
PC7		≥6 (LF)		•		
PC8	Add		•			
PR1		≥6 (L)		•		
PR2	⊠					
PR3				•		
PR4		≥6(S)		•		
PE1		≥6 (F)	•			before entry
				•		before & during entry
PE2	⊠					
PE3		≥6 (L)		•		
PE4	⊠					
PT1	⊠					
PT2	⊠					

Table A.4: Childrens' Books' Coverage of Official Guidelines (Left hand column refers to the numbers in Figure 3; •:agree, ⊗:conflicts with official)

	[53]	[44]	[45]	[46]	[48]	[52]	[47]	[55]	[56]	[51]	[49]	[50]	[54]	[58]	[57]
W1	•						•								•
W2		•					•		•			•	•		•
PI1							•								
PI2			•				•								•
PI3							•								
PI4										•					•
PI5	•	•									•		•		
PI6							•								•
PI7															
PI8															
PI9							•								
PLC1	•		•	•		•			•		•			•	
PC1															
PC2															•
PC3	⊗	⊗	⊗		⊗	⊗	⊗	⊗		⊗		•	⊗	⊗	⊗
PC4	•	⊗		•				•			•	•			•
PC5	•	•		•	•		•	•	•	•	•	•	•	•	•
PC6		•	•		⊗	•	•								
PC7			•												
PR1	•		⊗			•	⊗			•	•				
PR2							⊗								
PR3	•	•	•	•	⊗		⊗	•	•		•	•	•	•	•
PR4	•		•	•	•		•	•							•
PE1							•								
PE2															
PE3															
PE4							•								
PT1							•					•			
PT2												•			

Table A.5: Comparing Ontologies (O=Official, K=Kids, I=Online Advice) (•:agree, ⊗:conflicts with official, ≠:conflicting advice in different sources)

Why Passwords?	O	K	I
To Protect Valuable Assets	•	•	•
To Prove Identity	•		
Password Issues			
Shoulder Surfing	•	•	
Phishing	•	•	•
Keylogging	•	•	•
Social Engineering	•	•	
Password Guessing	•	•	
Someone Finding a Written Down Password	•	•	•
Forgetting a Password	•		
Network Sniffing	•		
Reused Password Cracked	•	•	
Password Leakage Consequences			
Impersonation	•	•	•
Password Creation			
Match Strength to Value	•		•
Use a Passphrase	•	≠	
Don't Choose Complex Passwords	•	⊗	⊗
Choose a Memorable Password	•	•	•
Don't Choose Predictable Passwords	•	•	•
Don't Reuse Passwords	•	•	•
Choose Easy to Type Passwords	•	•	
Password Retention			
Don't Write Passwords Down	•	⊗	•
Don't Change Regularly	•	⊗	⊗
Don't Share Passwords	•	≠	•
If Hacked, Change your Passwords	•	•	•
Password Entry			
Prevent Observation	•		
Verify URL before entering	•		•
Check for HTTPS before entering a Password	•		
Check for Physical Keylogger	•		•
Password Tools			
Password Managers	•	•	•
Two Factor Authentication	•	•	•

We, Suzanne Prior and Karen Renaud, declare that we have no conflict of interest with respect to manuscript number IJCCI-D-19-00001, titled *An Age-Appropriate Password "Best Practice'' Ontology for Early Educators and Parents.*